Department of Homeland Security Daily Open Source Infrastructure Report for 13 February 2009

Current Nationwide Threat Level is

ELEVATED
Significant Risk of Terrorist Attacks

For info click here
http://www.dhs.gov/

- According to the Associated Press, the Los Alamos nuclear weapons laboratory in New Mexico is missing 69 computers, including at least a dozen that were stolen last year. No classified information has been lost, a lab spokesman said. (See item **5**)
- The Associated Press reports that two big communications satellites collided 500 miles over Siberia in the first-ever crash of its kind in orbit. The collision involved an Iridium commercial satellite and a Russian satellite believed to be nonfunctioning. (See item **28**)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − [http://www.esisac.com]

1. *February 12, Associated Press* – (National) **High winds knock out power in South, East.** Wild wind with gusts sometimes reaching hurricane force has knocked out power to hundreds of thousands of customers from the Great Lakes to the East. About 255,000 customers were without power in Ohio alone. There were also about 52,000 outages in Michigan, more than 30,000 around Buffalo, New York, and about 80,000 in Pennsylvania. Outages are also reported in Tennessee, Kentucky, North Carolina, Indiana, Maryland, and other states.
   Source: http://www.msnbc.msn.com/id/29158553/

2. *February 12, Reuters* – (International) **Shell declares force majeure on Nigeria Bonny**

oil. Royal Dutch Shell said on February 11 that it had declared force majeure on its Nigerian Bonny oil shipments due to insecurity in the Niger Delta. "It was declared with effect 1800 hours on Tuesday due to logistics challenges related to the security situation in the area," a Shell spokesman in Nigeria said. "It will affect the remainder of February and perhaps March offtakes with some deferred to April," he said.
Source: http://www.reuters.com/article/rbssEnergyNews/idUSLC19084620090212

[Return to top]

Chemical Industry Sector

Nothing to report

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

3. *February 12, Reuters* – (Arizona) **APS Ariz. Palo Verde reactors to stay at full power.** Arizona Public Service will not have to shut the three reactors at the Palo Verde nuclear power station in Arizona following "engineering calculations" early on February 12, a spokesman for the company said. All three units were operating at full power early on February 12 and were expected to remain that way. On February 11, the company filed a report with the U.S. Nuclear Regulatory Commission that it was working to restore the operability of the atmospheric dump valves. The company declared the valves inoperable after engineering personnel discovered the backup nitrogen capacity, required to operate the valve to mitigate certain accident scenarios, was inadequate. The report said if actions to fix the problem were unsuccessful, the plant's technical specifications require all three units to be in hot shutdown by 7:18 p.m. on February 12. The spokesman said the engineers re-ran their calculations and determined earlier Thursday morning the safety margins built into the system were accurate — so the reactors will not have to shut.
Source:
http://uk.reuters.com/article/oilRpt/idUKN1243388620090212?pageNumber=1&virtualBrandChannel=0

4. *February 12, Brockton Enterprise* – (Massachusetts) **Pilgrim nuclear plant operating at reduced power.** The Pilgrim nuclear power plant was operating at 56 percent of capacity, according to information the company provides daily to the U.S. Nuclear Regulatory Commission. Power was reduced during the evening of February 11 while NStar repaired a problem with a transmission line in Auburn, said a spokesman for plant owner Entergy Corp. He said the plant has reduced its output from 685 megawatts to 450 megawatts until the repairs were completed so as not to overload the grid.
Source: http://www.enterprisenews.com/business/x188766740/Pilgrim-nuclear-plant-operating-at-reduced-power

[Return to top]

Defense Industrial Base Sector

5. *February 11, Associated Press* – (New Mexico) **69 computers missing from nuclear weapons lab.** The Los Alamos nuclear weapons laboratory in New Mexico is missing 69 computers, including at least a dozen that were stolen last year, a lab spokesman said. No classified information has been lost, a spokesman said. The watchdog group Project on Government Oversight on Wednesday released a memo dated February 3 from the Energy Department's National Nuclear Security Administration that said 67 computers were missing, including 13 that were lost or stolen in past 12 months. The lab was initiating a month-long inventory to account for every computer, the spokesman said. The computers were a cybersecurity issue because they may contain personal information like names and addresses, but they did not contain any classified information, he said. Also missing are three computers that were taken from a scientist's home in Santa Fe, New Mexico, on January 16, and a BlackBerry belonging to another employee was lost "in a sensitive foreign country," according to the memo and an e-mail from a senior lab manager.
   Source: http://www.google.com/hostednews/ap/article/ALeqM5g6QEPXqw-PCm21HnDYwg3sbGm5HAD969OPC81

[Return to top]

Banking and Finance Sector

6. *February 12, Associated Press* – (National) **Fugitive financier arrested at U.S. border.** An American fugitive accused in a $100-million mortgage fraud was caught at the Canadian border after taking a taxi from Toronto with $1-million in Swiss bank certificates and $70,000 stuffed in his shoes, authorities said yesterday. Authorities said the suspect also was carrying four ounces of platinum valued at more than $1,000 an ounce when he was arrested entering the United States at Buffalo, New York, on February 11. The suspect is the second of three fugitives to be caught in the investigation of Loomis Wealth Solutions, an investment company based in Roseville, California, and several related companies. Court documents say they had defrauded investors and mortgage companies of $100-million since 2006. The deals involved 500 homes and condominiums in California, Florida, Nevada, Illinois, Colorado and Arizona, Internal Revenue Service affidavits said. The suspect admits his guilt in an essay appearing online, and blames himself and his colleagues for helping to cause the U.S. financial meltdown by creating hundreds of millions of dollars in fraudulent mortgages that went bad. Until recently, the 27-year-old Sacramento man had been co-operating with investigators. But after posting the essay in which he admits his guilt on the Web site of a new mortgage-banking operation he was promoting called Triduanum Financial, the suspect fled.
   Source: http://www.theglobeandmail.com/servlet/story/LAC.20090212.FUGITIVE12/TPStory/International

7. *February 11, Computerworld* – (International) **Web site: More than 150 banks**

affected by Heartland data breach thus far. The number of financial institutions that have said they were affected by the data breach disclosed last month by Heartland Payment Systems Inc. is growing longer by the day and now includes banks in 40 states as well as Canada, Bermuda and Guam, according to the BankInfoSecurity.com news portal. The Web site on February 11 published a list containing the names of 157 institutions that it said have publicly disclosed to customers that they were victimized as a result of the breach at Heartland, a large payment processor in Princeton, New Jersey. The list includes two banks in Bermuda, plus one each in Canada and Guam. A Heartland spokesman said on February 11 that while he had seen the report on BankInfoSecurity.com, he was unable to verify whether the numbers cited by the Web site were correct. Meanwhile, in another indication of the fallout from the breach, 83 percent of the 512 banks that responded to an informal "quick poll" survey conducted in late January by the Independent Community Bankers of America (ICBA) trade group said that credit or debit cards they had issued were compromised in the incident at Heartland. Another 12 percent said they didn't know yet if they had been affected, while just 4 percent said they hadn't been, according to the ICBA, which has more than 5,000 member banks from around the United States. For the most part, the banks on the list compiled by BankInfoSecurity.com appear to be mostly smaller institutions — although there are a handful of larger ones, such as Sovereign Bank.
Source:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127822&intsrc=hm_list

8. *February 11, Reuters* – (National) **FDIC to extend bank debt backstop through October.** The Federal Deposit Insurance Corp (FDIC) will extend a guarantee program for about $1.4 trillion in bank debt and up to $500 billion in transaction deposit accounts through the end of October, U.S. regulators said. The Temporary Liquidity Guarantee Program, launched in October, 2008, to help boost confidence in U.S. credit markets, was due to expire at the end of June. In an interagency statement by regulators on February 11 following the announcement of the U.S. Treasury's revamped financial rescue plan, banking regulators said the FDIC would make the program available to banks for an additional four months in exchange for another premium. "The FDIC's Temporary Liquidity Guarantee Program has contributed importantly to the gradual easing of liquidity strains on our financial institutions," the regulators said in a statement. "Though funding conditions have eased somewhat, this temporary program will be extended for an additional four months to provide liquidity to our banks as part of this overall strategy to move our economy forward."
Source:
http://www.reuters.com/article/americasRegulatoryNews/idUSN1136799720090211

[Return to top]

Transportation Sector

9. *February 11, Idaho Mountain Express* – (Idaho) **Airport may try another 'approach.'** On Tuesday, February 3, the authority for Friedman Memorial Airport approved an airport manager's suggestion that a possible new electronic system be investigated, and

told him to return at the March monthly meeting with ideas on sources for funds to study the idea. The manager told the board an initial study probably would cost between $15,000 and $20,000. If pursued to completion, development and certification of the system by the Federal Aviation Administration (FAA) could cost up to $100,000. The proposed system is a satellite-linked GPS navigation system which could allow landing approaches when cloud ceilings are as low as 1,000 feet with 2.5 miles visibility. Aircraft would need only relatively inexpensive GPS receivers and displays to hook up to the system. Friedman has been struggling since 1994 to get certification of a $1 million, FAA-funded transponder landing system already installed at the airport. But the FAA, for unexplained reasons, has balked and the transponder landing system has been non-operational.
Source: http://www.mtexpress.com/index2.php?ID=2005124817

10. *February 11, Atlanta Journal-Constitution* – (Georgia) **Long airport lines 'all but eliminated.'** The hour-long security lines that for years have infuriated passengers at Hartsfield-Jackson International Airport might be a thing of the past. A $26 million security checkpoint expansion, better staffing by the Transportation Security Administration (TSA) and specially designated security lanes have reduced the number of waits longer than 20 minutes during the past three months. Ten new security gates opened at Hartsfield-Jackson about three months back — there are now 32 — and the airport added "black diamond" lanes to separate more experienced travelers from their less-traveled counterparts. The airport also opened "clear lanes" that cost passengers about $128 a year to use and are intended for business travelers. Statistics compiled by the airport indicate that the number of 20-plus-minute waits has declined. Despite a decrease in air traffic nationwide, December was a record year for Hartsfield-Jackson. The airport is the world's busiest, with 90 million passengers passing through its concourses last year. A TSA spokesman said that TSA, which got a new Atlanta head of operations last year, has increased its use of part-time workers to give the agency maximum scheduling flexibility. That allows TSA to swarm officers to specific gates during peak travel times.
Source: http://www.ajc.com/services/content/printedition/2009/02/11/airport0211.html

11. *February 11, Associated Press* – (Colorado) **Bridge fire shuts down 80-mile rail line in N Colo.** Fire damage to a Great Western Railway bridge has forced the temporary closure of an 80-mile line connecting Greeley, Windsor, Fort Collins, Loveland, Johnstown and Longmont, Colorado. The bridge is northwest of Greeley. The fire was reported Monday. The managing director of Great Western parent Omnitrax Inc. said it will take at least seven weeks to get materials before repairs can start. He said the railroad is working with its customers to find alternate transportation.
Source: http://www.krdo.com/Global/story.asp?S=9827234

[Return to top]

Postal and Shipping Sector

12. *February 12, Associated Press* – (Texas) **Unknown powder found in federal offices in Texas.** The FBI headquarters in El Paso was evacuated February 11 after two people in

the mail room were exposed to a white powdery substance in a letter that was addressed to a former Massachusetts governor and Republican Presidential candidate. An FBI spokeswoman said a field test showed the material found February 11 was not hazardous but more extensive tests are pending. The employees who came in contact with the powder were treated at the scene by emergency medical personnel. Everyone else in the federal law enforcement building, which houses about 200 FBI employees and nearly 100 U.S. Drug Enforcement Agency personnel, was sent home while hazardous materials crews worked to identify the substance. An FBI spokeswoman said the powder was in a piece of mail addressed to the Republican official with a return address of the FBI office in El Paso. She said that it appeared that the letter was sent to the FBI address after being returned as undeliverable.
Source: http://news.yahoo.com/s/ap/20090212/ap_on_re_us/fbi_powder_scare

13. *February 11, Cincinnati Enquirer* – (Ohio) **White powder mailed to Clermont office.** Clermont County employees have been warned to be careful opening mail after an envelope addressed to a local government office was found to contain a suspicious white powder. The substance was discovered in an envelope addressed to a Clermont County office, which has some mail delivered to and sorted at a US Bank facility in the Linwood neighborhood of Cincinnati, an FBI agent said. The Cincinnati Fire Department's hazardous materials team responded and analyzed the powder. "The preliminary tests on the powder, which was inside the letter, (showed) there was no dangerous material," said the FBI official. "No one at the scene showed any sign of any reaction to any type of harmful substance." The letter has been sent to the Ohio Department of Health's Laboratory Response Network for further analysis. FBI and U.S. Postal Service inspectors are investigating.
Source: http://news.cincinnati.com/article/20090211/NEWS01/302110065

14. *February 9, Rocky Mountain Telegram* – (Colorado) **Authorities: Powder found in mailbox not a health threat.** Colorado state and local emergency officials are continuing to investigate after a suspicious powder was found on February 9 inside a Rocky Mount mailbox, although initial tests indicate the substance was not hazardous. Crews worked on scene for several hours to identify the white powder discovered inside a residential mailbox in the Sportsman Trail subdivision, before sending a sample of the substance to Greenville for testing. Authorities quarantined the area shortly after the powder was reported at 1 p.m., but officials said late on February 9 that it did not seem as if the substance posed a health threat. The Rocky Mount Fire Department was joined in responding by Nash County Emergency Services and the Rocky Mount Police Department. Officials with the Nash County Division of Emergency Management were notified and placed on standby.
Source: http://www.rockymounttelegram.com/news/authorities-powder-found-in-mailbox-not-a-health-threat-424263.html

[Return to top]

Agriculture and Food Sector

15. *February 12, Associated Press* – (Georgia) **Ga. panel OKs food safety changes after**

outbreak. A sweeping new food safety measure proposed in the wake of the salmonella outbreak easily passed its first key legislative hurdle on February 11 as Georgia lawmakers sought to reassure antsy residents. The Senate Agriculture Committee unanimously approved a plan that would require food makers to alert state inspectors within 24 hours if a plant's internal tests show its products are contaminated. State law did not require the company to share those test results, and state officials say they may have been able to stop the outbreak if they'd known about them sooner. Food safety experts, government groups and industry lobbies say they don't know of any other state that requires food manufacturers to share internal data. The Peanut Corp. faces a growing number of civil lawsuits and federal authorities have launched an investigation. Georgia lawmakers, also eager to show they are probing the outbreak, have set up committees and proposed legislation to tweak the state food network. The bill, which now goes to the full Senate, also empowers Georgia agriculture officials to order plants to have their products tested at their own expense. And it allows state officials to set policy guiding how often the plants should test. The proposal would exempt meat, poultry and other manufacturers under the U.S. Department of Agriculture's watch. Instead, it focuses on the thousands of other plants focused on the Food and Drug Administration's scrutiny.
Source: http://www.businessweek.com/ap/financialnews/D96A436G1.htm

16. *February 11, Brownfield Network* – (California) **Please, do not dump those bull calves.** Low milk prices have made bull dairy calves of no value on the market and that has prompted fears that some are just dumping the calves. Farm Sanctuary is offering a $2,000 reward for information leading to the identification and arrest of the person or people responsible for dumping 30 dead calves in San Joaquin County, California last month. Officials say they have found nearly 50 dead calves dumped in the county over the past two months. The fear is there will be more of these incidents across the country as dairy prices plunge. Dairy industry leaders are appealing to producers to avoid any such action.
Source: http://www.brownfieldnetwork.com/gestalt/go.cfm?objectid=6768FFE0-5056-B82A-D0082D10BFF778F3

17. *February 11, Food Production Daily* – (Maryland) **Maryland eyes artificial food color ban.** Maryland could become the first U.S. state to ban several artificial food colorings which have been linked to hyperactivity and behavioral problems in children, if proposed legislation is approved. Two bills are scheduled to be considered at hearings in Annapolis on February 11, including one that would require food manufacturers to add a warning label prior to an outright ban in 2012, and another that would prohibit the use of the colors in school foods. If the legislation is approved, food products containing the colors would be required to carry the label: "Warning: The color additives in this food may cause hyperactivity and behavior problems in some children" effective from January 1, 2010, and be phased out by December 31, 2011. The Center for Science in the Public Interest (CSPI) has given its backing to the bills, which were introduced by a Senator, and a CSPI senior nutritionist who has said that he will testify at the hearings in favor of their adoption.
Source: http://www.foodproductiondaily.com/Publications/Food-Beverage-

Nutrition/FoodNavigatorUSA/Legislation/Maryland-eyes-artificial-food-color-ban/?c=DtqJR18k3PmFGYrXgqjpeQ%3D%3D&utm_source=newsletter_daily&utm_medium=email&utm_campaign=Newsletter%2BDaily

18. *February 10, Produce Traceability Initiative* – (Maryland) **Produce groups unveil traceability resource site.** A new Web site aims to provide tools to help the industry put in place measures proposed by the joint Produce Traceability Initiative (PTI). The site, www.producetraceability.org, is a joint effort of the Newark, Delaware-based Produce Marketing Association (PMA), the Ottawa-based Canadian Produce Marketing Association (CPMA), and the Washington, D.C.-based United Fresh Produce Association. The PMA, CPMA and United Fresh announced the launch of the Web site on February 9. The site includes a list of more than 40 companies which have signed on in support of the PTI. The initiative's steering committee issued recommendations for the industry to move to a common standard for electronic produce traceability by the end of 2012, the news release said. The release said the system, when implemented, could substantially narrow the impact of product recalls. The director of industry technology and standardization for CPMA noted that the fundamental difference between Canada and the United States regarding the PTI is that Canadian retailers have decided they are not going to pursue the same timeline put forward by the PTI.
Source: http://www.thepacker.com/icms/_dtaa2/content/wrapper.asp?alink=2009-122756-877.asp&stype=topnews&fb

[Return to top]

Water Sector

19. *February 11, Evansville Courier Press* – (Indiana) **Breaks blanketing city.** Roughly 100 Evansville water mains have broken since the January 26 ice storm, prompting boil orders and traffic delays citywide. Harsh winter weather and cold water temperatures in the Ohio River have placed intense pressure on the city's water mains, said the general manager of the Evansville Water and Sewer Utility. Widespread breaks are common when the temperature of the Ohio River dips into the 40-degree range. The ground temperature is typically about 58 degrees. The cold water adds stress to the pipes, which attempt to stabilize the contrasting temperatures, he said. The city's water mains range in size from 2 to 48 inches, he said. The smaller pipes feed into larger ones called transmission mains. Most of the damage has been to the mains 24 inches and smaller. The average life span of a water main is 20 years, but some in downtown are up to 60 years old. With the Ohio River expected to stay cold for weeks to come, the manager expects more mains to fail.
Source: http://www.courierpress.com/news/2009/feb/11/breaks-blanketing-city-damage-extensive/

20. *February 11, Waste News* – (Pennsylvania) **Del Monte fined for wastewater violations at Pa. plant.** Del Monte Corp. is being fined nearly $3,500 for industrial wastewater violations last fall at a plant in South Centre Township, Columbia County, Pennsylvania. The Pennsylvania Department of Environmental Protection (DEP) said the food company took its wastewater lagoon out of service last year to replace a torn

liner. But the firm's interim treatment plan was not approved by the DEP and resulted in 20 instances where the company exceeded its discharge permit limits. Del Monte received a new water quality management permit from the DEP on January 27 to modify and repair the lagoon.
Source:
http://www.wasterecyclingnews.com/headlines2.html?id=1234365977&allowcomm=true

21. *February 10, Spokesman-Review* – (Idaho) **Rathdrum Prairie board looks to increase wastewater irrigation.** A 55-acre grove of hybrid poplar trees grown by the Hayden Area Regional Sewer Board are cultivated for their spongelike roots. During the summer, the poplars and adjacent fields of alfalfa and orchard grass soak up 1.2 million gallons of treated wastewater daily, said the sewer board's manager. The irrigation keeps the effluent out of the Spokane River, where it would nourish noxious algae blooms. Instead, the nutrient-rich wastewater helps fertilize crops. The system could become a prototype for other Idaho cities. Irrigating 4,000 acres on the prairie with treated wastewater might help solve the long-term sewage disposal needs of Post Falls, Hayden and Rathdrum, according to the Rathdrum Prairie Wastewater Master Plan.
Source: http://www.spokesman.com/stories/2009/feb/10/rathdrum-prairie-board-looks-increase-wastewater-i/

[Return to top]

Public Health and Healthcare Sector

22. *February 11, SC Magazine* – (National) **Medical data leakage rampant on P2P networks.** The risk of patient information disclosures on peer-to-peer (P2P) networks is much higher than if a health care worker loses a laptop or removable storage device, according to new Dartmouth College research. A Dartmouth College business professor has written a report called "Data Hemorrhages in the Health Care Sector" and plans to present his findings later this month at the Financial Cryptography and Data Security conference. P2P networks are Internet-based file sharing networks that allow users to share music or other files — LimeWire or BearShare are popular examples. Over a two-week period, Dartmouth College researchers, in collaboration with P2P monitoring vendor Tiversa, searched file-sharing networks for key terms associated with the top ten publicly traded health care firms in the country, and discovered numerous sensitive documents — for example, a spreadsheet from an AIDS clinic with 232 client names, including Social Security numbers, addresses and birthdates. The researchers also discovered databases for a hospital system that contained detailed information on more than 20,000 patients, including Social Security numbers, contact details, and insurance records, along with diagnosis information.
Source: http://www.scmagazineus.com/Medical-data-leakage-rampant-on-P2P-networks/article/127216/

23. *February 11, HealthDay News* – (National) **Key to Lyme disease virulence discovered.** BmtA, a protein that is essential for the bacterium that causes Lyme disease to become virulent, has been identified by microbiologists at the University of Texas

Southwestern Medical Center at Dallas. The researchers said their finding may help lead to new methods of fighting the tick-borne infection. This bacterial protein aids in transporting the metal manganese from a host tick or mammal to the Lyme-disease causing bacterium Borrelia burgdorferi. The study was published in this week's online issue of the Proceedings of the National Academy of Sciences.
Source: http://www.healthday.com/Article.asp?AID=623949

24. *February 11, Global Security Newswire* – (Kansas) **Biodefense research could move to Kansas early, DHS says.** The United States might conduct biological defense research at Kansas State University before a new laboratory is built there for that purpose, the U.S. Homeland Security Secretary said February 9. Construction of the $450 million National Bio- and Agro-Defense Facility is expected to start next year and continue for roughly five years, the Associated Press reported. The laboratory would replace the Plum Island Animal Disease Center in New York. She did not specify what research could be conducted at the university or how soon it might begin. Appearing at a press conference with the Secretary, Kansas's governor said that Homeland Security could purchase or lease the university's Biosecurity Research Institute.
Source: http://www.globalsecuritynewswire.org/gsn/nw_20090211_4394.php

[Return to top]

Government Facilities Sector

Nothing to report

[Return to top]

Emergency Services Sector

25. *February 10, North Adams Transcript* – (Massachusetts) **Massachusetts rescuers build item they couldn't buy.** A piece of life-saving equipment that would have cost the North Adams Fire Department about $3,500 wound up costing only $500 with a little ingenuity and some help form the community. The fire department debuted its new Wilderness Rescue All-Terrain Transport (WRATT) at Windsor Lake on Monday. The WRATT is an off-road sled that can be hooked up to a four-wheeler or snowmobile to transport patients from isolated areas. The WRATT was hand-built by a local firefighter, who has fabrication experience, after the local fire director saw that a commercially available unit was too expensive. The director said the WRATT was a huge improvement over the old way of transporting a patient from a wooded area.
Source: http://www.emsresponder.com/article/article.jsp?id=8971&siteSection=12

[Return to top]

Information Technology

26. *February 11, CNET News* – (International) **Hacker site claims breach of third security firm Web site in a week.** A Romanian hacker site said on February 11 it was

able to breach the Web site of Helsinki-based security firm F-Secure just as it had gained access to the sites of two other security companies recently. F-Secure is "vulnerable to SQL Injection plus Cross Site Scripting," an entry on the HackersBlog site said. "Fortunately, F-Secure doesn't leak sensitive data, just some statistics regarding past virus activity." An F-Secure spokesman said the company had taken the affected server down and that it was a low-level server that was not critical to the company and had no sensitive or customer data on it, just statistical data for marketing purposes. HackersBlog publicized on its site that it had breached the U.S. Web site of Moscow-based firm Kaspersky on February 7 and the Portugal site of BitDefender on February 9 using the same attack techniques.
Source: http://news.cnet.com/8301-1009_3-10161874-83.html?part=rss&tag=feed&subj=News-Security

27. *February 11, DarkReading* – (International) **New and improved Storm botnet morphing Valentine's malware.** The botnet formerly known as Storm is ramping up its ability to evade detection by automatically generating thousands of different variants of its malware each day as it spreads and recruit more bots. Waledac, the new and improved Storm, is using its favorite holiday, Valentine's Day, to spread the love with signature phony greeting cards and romance-themed email that Storm so infamously spread in the past. "Over the last 24 hours, we've seen over 1,000 new variants [of Waledac code]," said a senior researcher with Eset, which expects Waledac to eventually pump out thousands of variants a day. "It was a bit lower than what we are expecting. It may not have reached many of our clients yet." That said, it's still a big jump from the around 10 new versions a day Eset had seen the botnet creating, he adds. One of Waledac's latest attacks comes in the form of a puppy love e-card with a Valentine's-related link, as well as other warm and fuzzy-looking email. Subject lines include the usual "a Valentine card from a friend" and "you have received a Valentine E-card," but once you click the URL to retrieve the message, Waledac's malware is downloaded onto your machine. Another attack uses a phony pop-up that appears to be from Microsoft stating the machine is infected with spyware. That leads to a fake antispyware site that not only infects the machine, but also tries to sell the victim its scareware, according to the director of product management for Marshal8e6.
Source: http://www.darkreading.com/security/attacks/showArticle.jhtml;jsessionid=OSFS5MKSLIVSOQSNDLRSKH0CJUNN2JVN?articleID=213403915

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: http://www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Communications Sector

28. *February 11, Associated Press* – (International) **Satellites collide 500 miles over Siberia.** Two big communications satellites collided in the first-ever crash of its kind in orbit, shooting out a pair of massive debris clouds and posing a slight risk to the international space station. NASA said it will take weeks to determine the full magnitude of the crash, which occurred nearly 500 miles over Siberia on February 10. "We knew this was going to happen eventually," said an orbital debris scientist at Johnson Space Center in Houston. NASA believes any risk to the space station and its three astronauts is low. It orbits about 270 miles below the collision course. There also should be no danger to the space shuttle set to launch with seven astronauts on February 22, officials said, but that will be re-evaluated in the coming days. This was the first high-speed impact between two intact spacecraft, NASA officials said. The collision involved an Iridium commercial satellite, which was launched in 1997, and a Russian satellite launched in 1993 and believed to be nonfunctioning. The Russian satellite was out of control, the scientist said. Iridium Holdings LLC has a system of 65 active satellites that relay calls from portable phones that are about twice the size of a regular mobile phone. It has more than 300,000 subscribers. The U.S. Department of Defense is one of its largest customers. The company said the loss of the satellite was causing brief, occasional outages in its service and that it expected to have the problem fixed by February 13.
Source: http://www.huffingtonpost.com/2009/02/11/2-big-satellites-collide-_n_166214.html

29. *February 11, DarkReading* – (International) **New vulnerability found in BlackBerry's Web application loader.** BlackBerry maker Research In Motion this week is warning users about a newly discovered vulnerability that could potentially enable an attacker to gain remote control of the device or crash its browser. The flaw was found in the BlackBerry's Web Application Loader, an ActiveX feature that enables the handheld to load new applications via the Internet Explorer browser. RIM says that "an exploitable buffer overflow" exists in the BlackBerry Application Web Loader ActiveX control. According to an advisory issued by US-CERT, the flaw may be exploited by phishers or other attackers. "By convincing a user to view a specially crafted HTML document, an attacker may be able to execute arbitrary code with the privileges of the user," the advisory says. "The attacker could also cause Internet Explorer to crash." US-CERT says the vulnerability has been assigned a Common Vulnerability Scoring System rating of 9.3 on a 10-point scale, which means the vulnerability is highly dangerous and potentially easy to exploit. RIM says users can eliminate the vulnerability by uploading the current, patched version of Web Application Loader, which does not have the flaw. Users can also disable the ActiveX control in their current browsers, the company says.
Source: http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=213900073

[Return to top]

Commercial Facilities Sector

30. *February 12, Statesman Journal* – (Oregon) **Suspicious packages disrupt Lancaster Mall.** A portion of Lancaster Mall was evacuated February 11 for several hours while Salem police investigated three reported suspicious devices, none of which turned out to be a threat, police said. The first package was reported by mall security about 10:30 a.m. near the Macy's department store doors. The bomb squad cordoned off the Macy's parking lot and evacuated the store, adjacent stores in the mall and eventually Sports Authority. The bomb squad's robot inspected the first package, which appeared to be a suitcase left in the shrubbery. The robot destroyed the suitcase. Meanwhile, two more suspicious packages were found as officers checked the area. Both turned out to be harmless. One was a black plastic bag with leaves inside, police said. Lancaster Mall was reopened by 1:15 p.m. By 1:30 p.m., business resumed as normal, the Lancaster Mall manager said.
Source: http://www.statesmanjournal.com/article/20090212/NEWS/902120359/1001
See also: http://www.kptv.com/news/18692353/detail.html

31. *February 12, San Mateo Daily Journal* – (California) **Bomb squad detonates device.** Police are investigating whether an explosive device found at a Redwood City apartment February 11 was planted by someone who once stayed with the resident, a Redwood City police captain said. Redwood City police responded to a report of a suspicious package in an apartment at approximately 4:39 p.m. February 11. Responding officers determined the fabric-like cylinder contained explosive material and called the San Mateo County Bomb Squad. The woman at the apartment reportedly received the suspicious device at approximately 3:30 p.m., but waited an hour before calling police. She took the device in and out of her purse several times and eventually left it on her porch before calling 911, police said. The apartment complex and area around the apartment was evacuated. The bomb squad examined and detonated the device on the woman's porch. This process caused minor damage to the wall outside the apartment's living room. There were no injuries related to the incident, police said. The incident is currently under investigation by the Redwood City Police Department.
Source: http://www.smdailyjournal.com/article_preview.php?id=105539

32. *February 11, Guardian.co.uk* – (International) **Climate Camp to target the city in summer protest.** The organizers of Climate Camp, a protest group that has previously demonstrated at coal power stations and Heathrow airport, have chosen London's financial center as the target of their main summer protest this year. The decision to target the city is aimed at throwing a spotlight on the carbon trading system, one of the central planks of the European Union's attempts to reduce carbon dioxide emissions from businesses. Carbon trading in the United States is also being pushed by the current Administration, but the activists say they want to highlight the failure of the mechanism to reduce greenhouse gas emissions. The precise form of the protest and where it will take place are yet to be decided. Climate Camp is organized by consensus, so there must be unanimous agreement about the final decision. So far, no decision has been made about where exactly the camp itself will be or when it will take place, although rural locations in and around London are being considered, along with London parks. The

group is organizing a separate protest in the city on April Fools' Day on the eve of the G20 leaders' summit in London.
Source:
http://www.guardian.co.uk/environment/2009/feb/11/emissionstrading-carbonemissions

33. *February 11, Associated Press* – (National) **Officials offer assurances after radioactive find in Belfast.** Authorities removed some radioactive material and instructions for building a "dirty bomb" from the Belfast, Maine home of a man whose wife is accused of fatally shooting him. Law enforcers said February 11 there was never a public health risk. The radioactive materials discovered in the home after the man was killed on December 9 were not enough to make a dirty bomb, officials said. A National Guard civil team went to the home after the shooting, and a state hazardous materials team removed several items, officials said February 11. The Bangor Daily News reported February 11 that four small jars of depleted uranium, a byproduct of the uranium enrichment process, and thorium 232, another radioactive material, were discovered in the home, along with other chemical compounds and four one gallon containers of 35 percent hydrogen peroxide. The newspaper cited a report by the Washington Regional Threat and Analysis Center that had been leaked online. The center confirmed the document's authenticity to the Associated Press. The Bangor Daily News reported that Maine has its own fusion center, but the reason the man ended up on the D.C. center's radar is because his threats had the potential to affect the Presidential Inauguration, a spokeswoman for the center said. Unlike a nuclear bomb, a dirty bomb is created with conventional explosives used to scatter radiation and create fear among a population.
Source:
http://www.fosters.com/apps/pbcs.dll/article?AID=/20090211/NEWS0104/902119879.
See also: http://www.bangornews.com/detail/99310.html

[Return to top]

National Monuments & Icons Sector

34. *February 12, National Parks Traveler* – (North Carolina) **Ginseng poachers at Great Smoky Mountains National Park receive jail time.** Poaching "sang" in Great Smoky Mountains National Park rewarded two North Carolina men with time in jail and fines. "Sang" is slang for ginseng, an herb that grows in Eastern forests and is valued by many for its supposed curative, and supposed aphrodisiacal, powers. A 24-year-old man from Canton, North Carolina, and a 46-year-old man of Clyde, North Carolina, were convicted and sentenced in federal court on January 22. The older of the two was convicted of illegally digging American ginseng, and both were convicted for failure to obey a lawful order given by a U.S. Park Ranger, according to park officials. Illegal harvest of plants is a serious problem in Great Smoky Mountains National Park. Ginseng poaching is a particular problem, as the plant's root commands a high price in the black market. Illegal digging has increased over the years and has put pressure on the plant's survival.
Source: http://www.nationalparkstraveler.com/2009/02/gingseng-poachers-great-smoky-mountains-national-park-receive-jail-time

[Return to top]

Dams Sector

35. *February 12, Southern Illinoisan* – (Illinois) **To dam or not to dam?** The future of Cache River's swamp drainage is being questioned because of a court dispute between the Illinois Department of Natural Resources (IDNR) and the Big Creek Drainage District. On Friday, a judge ruled in a preliminary injunction the dam be taken down and set a hearing set for February 26. IDNR reinstated the dam in April after it had been taken down by the Big Creek Drainage District. Both sides are afraid of damage. Those who favor leaving the dam up are concerned with how a change will affect the wildlife. Those who favor taking it down worry about the water's effect on hardwood trees in the area.
Source: http://www.southernillinoisan.com/articles/2009/02/12/front_page/28184375.txt

36. *February 12, Charlotte Observer* – (North Carolina) **NC investigating contaminated fish.** The North Carolina Division of Water Quality will investigate the source of contaminated fish in Badin Lake east of Charlotte, an official said Wednesday. State health authorities have posted a fish-consumption advisory for largemouth bass and catfish caught in the lake. Those species may be contaminated by polychlorinated biphenyls, or PCBs. Badin Lake becomes the third North Carolina body of water — the other two are near Raleigh — where consumers have been warned of eating PCB-contaminated fish. Advisories for the toxic metal mercury are more widespread, covering certain species of fish across Eastern North Carolina, and largemouth bass statewide. The Badin advisory was posted as aluminum-maker Alcoa spars with Stanly County over water rights and contamination from its now-closed smelter on Badin Lake. As part of the company's renewal of its 50-year federal hydroelectric license for the Yadkin River, the state water-quality division has to certify that Alcoa's dams and lakes will not hurt the Yadkin. The state has until May to issue the permit.
Source: http://www.charlotteobserver.com/breaking/story/532018.html

37. *February 11, Kent Reporter* – (Washington) **City officials keep close watch on Howard Hanson Dam.** Kent city officials are keeping a close watch on the drop in storage capacity at the Howard Hanson Dam because of the potential impact of valley flooding from the Green River if a severe rainstorm strikes. Kent Valley residents, businesses and property owners are slated to receive an informational letter this week from the town mayor in connection with the decision by the U.S. Army Corps of Engineers to lower the storage level because of a damaged abutment at the dam. The Army Corps operates the dam, about 20 miles east of Kent, to help control the level of the Green River as it flows through Auburn, Kent, Tukwila and Renton. Corps engineers found a damaged abutment at the dam after the heavy rainfall in early January and decided to lower storage capacity at the dam's reservoir until they can fix the problem. "There is no immediate danger to people or property below the dam," said the spokeswoman for the Seattle division of the U.S. Army Corps of Engineers in a phone interview Thursday. "The damage is not in the dam itself, but the abutment." The emergency management services division of the Kent Fire Department will work with

the Army Corps, Red Cross, King County, and the cities of Auburn, Renton and Tukwila to prepare for a major flooding event, said the Kent assistant fire chief, in a report to the city council. He said the cities will develop a flood-warning system, figure out a potential evacuation of residents and where to shelter those people.
Source: http://www.pnwlocalnews.com/south_king/ken/news/39395759.html

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.
To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer